



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/879,575	06/12/2001	James Alexander Reeds III	037-0039	4755

52218 7590 10/22/2007
ZAGORIN O'BRIEN GRAHAM LLP (037)
7600B NORTH CAPITAL OF TEXAS HIGHWAY
SUITE 350
AUSTIN, TX 78731-1191

EXAMINER

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

MAIL DATE	DELIVERY MODE
-----------	---------------

10/22/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/879,575

Applicant(s)

REEDS ET AL.

Examiner

Ellen C. Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 August 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 5-16, 18-22, 26-35, 37-43 and 45-57 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3, 5-16, 18-22, 26-35, 37-43 and 45-57 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Ellen C. Tran
ELLEN TRAN
PATENT EXAMINER
ART 2134

DETAILED ACTION

1. This action is responsive to communication: filed on 15 August 2007 with acknowledgement of an original application filed 12 June 2001.
2. Claims 1-3, 5-16, 18-22, 26-35, 37-43, and 45-57, are currently pending in this application. Claims 1, 14, 33, 41, 48, 49, and 53 are independent claims

Response to Arguments

3. Applicant's arguments filed 13 August 2007 have been fully considered but they are moot due to new grounds of rejection where noted below or not persuasive.

I) In response to Applicant's argument beginning on page 12, *"Nowhere does Schneier teach or suggest that limitation of claim 1 ... 14, 41, 49, 53, ... Medvinsky fails to compensate for the shortcomings of Scheier ... Nowhere does Medvinsky teach or suggest selecting a fixed length segment of a continuous decryption key stream based on a received session count of data packet, as required by claim 1"*.

The Examiner disagrees with argument presented and notes the following. The below rejection has been changed because Medvinsky alone teaches the aspects of claim 1. As is known a stream cipher is an XOR operation based on fixed length segment (i.e. keystream), Medvinsky teaches the use of a stream cipher, therefore the Schneier is unnecessary. Furthermore Medvinsky teaches the selection of the fixed length segment based on a session count. Although the wording in Medvinsky is not the same as applicant claims the teaching is the same. A Real Time Protocol (RTP) is well known in the art that RTP services include: Payload-type identification, Sequence number, Time stamping, and Delivery monitory. Therefore this along with the teaching of Medvinsky is interpreted to mean that the keystream is

synchronized according to the sequence number, time stamping, and delivery conditions. Note sequence number, time stamp, or delivery condition can be interpreted as a 'session count'.

II) In response to Applicant's argument beginning on page 13, *"Regarding claim 48, Applicants respectfully maintain that Schneier, alone or combination with Medvinsky, or other references of record fails to teach or suggest a session count evaluator configured to determine if a difference between a received session count within the encrypted data packet and a locally generated session count is less than a threshold ... Nowhere does Medvinsky teach session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and locally generated session count is less than a threshold, as required by claim 48"*.

The Examiner disagrees with argument presented and notes the following. The Medvinsky references should be reviewed for all it contains. Using the Real Time Protocol (RTP) the packets are inherently evaluated for session counts that are not synchronized. This is shown in Medvinsky paragraphs 0033-0035 and 0053.

III) In response to Applicant's argument beginning on page 18, *"Claim Rejection Under 35 U.S.C. §103 Over Schneier in View of Jung Claims 7-13, 26-35, 37-40, and 48-51 stand rejected ...Regarding claim 33, Applicants respectfully maintain that Schneier, alone or in combination with Jung, or other references of record, fails to teach or suggest a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold"*.

The Examiner disagrees with argument presented and notes the following. The below rejection has been changed because Medvinsky alone teaches the aspects of claim 33. The

Art Unit: 2134

Medvinsky references should be reviewed for all it contains. Using the Real Time Protocol (RTP) the packets are inherently evaluated for session counts that are not synchronized. This is shown in Medvinsky paragraphs 0033-0035 and 0053.

IV) In response to Applicant's argument beginning on page 23, "*Claim Rejection Under 35 U.S.C. §103 Over Schneier in View of Medvinsky and Sengodam Claims 54-57 stand rejected ... Applicants respectfully maintain that Schneier, alone or in combination with Medvinsky, Jung, Sengodam, and/or other references of record, fails to teach or suggest padding the payload to a given size with padding, the given size correspond to the fixed length segment size, wherein the fixed length segment of the continuous decryption key is applied both padded payload, a remaining portion of the fixed length segment being applied to the padding*" ... *The amount of padding of Sengodan is variable and fails to teach or suggest padding the payload to a given size with padding, the given corresponding to the fixed length segment size, as required by claim 54*".

The Examiner disagrees with argument presented and notes the following. It is well known that padding is added to a payload in order make the packets a fixed length.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2134

5. **Claims 1-3, 5-8, 14-16, 18-22, 26, 27, 33-35, 37-39, 41-43, 45-51, and 53** are rejected under 35 U.S.C. 102(e) as being anticipated by Medvinsky U.S. Patent Application Publication No. 2002/0094081 (hereinafter '081).

As to independent claim 1, "A method comprising: selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet" is taught in '081 pages 3-4 paragraphs 0033-0034;

"and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet" is shown in '081 page 2, paragraphs 0017-0018.

As to dependent claim 2, "wherein the applying comprises performing a bit per bit streaming encryption process" is disclosed in '081 page 3, paragraph 0034.

As to dependent claim 3, "wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet" is taught in '081 page 3, paragraph 0034.

As to dependent claim 4, "wherein the applying further comprises performing an RC4 operation with the portion of the fixed length segment and the data packet" is shown in '081 page 3, paragraph 0034.

As to dependent claim 5, "further comprising: receiving the data packet, the data packet comprising at least a portion of the received session count" is shown in '081 page 2, paragraphs 0017-0018.

As to dependent claim 6, "wherein the data packet further comprise at least a portion of a received message digest value" is disclosed in '081 page 4, paragraph 0054.

As to dependent claim 7 “wherein the selecting comprises: selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value” is shown in ‘081 page 4, paragraphs 0036-0051.

As to dependent claim 8, “wherein the selecting further comprises: extracting the at least a portion of the received session count from the encrypted data packet; expanding the at least a portion of the received session count to the received session count; and comparing the received session count to the locally generated session count” is disclosed in ‘081 pages 3-4 paragraphs 0033-0034.

As to independent claim 14, “A method of generating an encrypted data packet, the method comprising: selecting a fixed length segment of a continuous encryption key stream” is taught in ‘081 pages 3-4 paragraphs 0033-0034;

“applying a portion of the fixed length segment to data to form an encrypted payload; generating a session count based in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet” is shown in ‘081 page 2, paragraphs 0017-0018.

As to dependent claims 15, 16, and 17, these claims contain substantially similar subject matter as claims 2, 3, and 4; therefore they are rejected along the same rationale.

As to dependent claim 18, “further comprising: generating a message digest value; and combining at least a portion of the message digest value with the encrypted payload to form the encrypted data packet” is taught in ‘081 page 4, paragraphs 0054 –0055.

As to dependent claim 19, “wherein the generating comprises: generating the message digest value based on the encrypted payload, the session count and a message digest key” is shown in ‘081 page 4, paragraphs 0054 –0055.

As to dependent claim 20, “further comprising: forming the at least a portion of the message digest value by truncating the message digest value” is disclosed in ‘081 page 4, paragraphs 0054 –0055.

As to dependent claim 21, “further comprising transmitting the encrypted data packet to a receiver through a communication channel” is taught in ‘081 page 2, paragraph 0016.

As to dependent claim 22, “further comprising: receiving a received data packet corresponding to the encrypted data packet, the received data packet comprising the encrypted payload, at least a portion of a received session count and a received truncated message digest value; selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet” is shown in ‘081 pages 3-4 paragraphs 0033-0034 and page 4, paragraphs 0053-0055.

As to dependent claims 23-27, these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 33, “A receiver comprising: a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold” is taught in ‘081 pages 3-4 paragraphs 0033-0034;

“and a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold” is shown in ‘081 page 2, paragraphs 0017-0018.

As to dependent claims 34-39 these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 41, this claim is directed to a transmitter of the method of claim 14; therefore it is rejected along similar rationale.

As to dependent claims 42-51, these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 48, is directed to a system consisting of independent claims 33 and 41; therefore it is rejected along the same rationale.

As to independent claim 49, **“A method comprising: receiving a data packet through a communication channel”** is taught in page 2, paragraph 0016;

“the data packet comprising at least a portion of a session count; selecting a fixed length segment of a continuous decryption key stream based on the session count” is taught in ‘081 pages 3-4 paragraphs 0033-0034;

“and applying a portion of the fixed length segment by performing a bit per bit streaming encryption to decrypt a payload of the data packet” is shown in ‘081 page 2, paragraphs 0017-0018.

As to dependent claims 50 and 51, these claims contain substantially similar subject matter as claims 7 and 8; therefore they are rejected along the same rationale.

As to independent claim 53, “A method of generating an encrypted data packet, the method comprising: selecting a fixed length segment of a continuous encryption key stream” is taught in ‘081 pages 3-4 paragraphs 0033-0034;

“applying a portion of the fixed length segment to data by performing a bit per bit streaming encryption process to form an encrypted payload; generating a session count in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet” is shown in ‘081 page 2, paragraphs 0017-0018.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. **Claims 9-13, 28-32, 40, and 52**, are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘081 in further view of Chang et al. U.S. Patent 6,105,012 (hereinafter ‘012).

As to dependent claim 9, “**further comprising: discarding the data packet if the difference is not less than the threshold value**” however ‘012 teaches “The key check block is sent to the receiver as a header of the current encrypted data payload. The receiver also retains the last eight bytes of the current packet, it decrypted the first eight bytes (the key check block) and compares the result to the retained last eight bytes ... If there is no match, an error occurred and the receiver takes appropriate action” on page 5, paragraph 0052.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method key selection for decryption taught in '081 to include a means to compare the keys being used and take appropriate action (i.e. delete packet) when a match is not found. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to protect data during transmission see '012 (page 1, paragraphs 0005-0006). "It is known to remedy this deficiency by decrypting the data field of the packet with the current session key, as well as the next key in the sequence of keys, and choose the key for which the decrypted data makes sense. Using this method, the change-over from one session key to the next is automatically detected. However, to determine whether the decrypted data makes sense requires knowledge about the information being transmitted. This is not always the case, limiting the use of this method. It is an object of the invention to provide a secure communication system, sink device and secure communication method which overcome above mentioned drawback".

As to dependent claim 10, "further comprising: re-synchronizing a decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the difference in not less than the threshold value" is taught in '081 page 4, paragraphs 0041- 0053 "it signals the CODEC change to gateway controller 106. MTA 104 generates a new set of RTP key stream and a new initial time stamp. Herein lies a first advantage of the present invention. The related art provides for re-derivation of the RTP key stream when a CODEC change occurs, by providing the following key derivation function ... "End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function".

As to dependent claim 11, “further comprising: discarding the data packet if the at least a portion of the received message digest value does not match a locally generated message digest value” is taught in ‘012 page 5, paragraph 0052-0053.

As to dependent claim 12, “further comprising: re-synchronizing the decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value” is shown in ‘081 page 4, paragraph 4-5, paragraphs 0054-0057 “In a further embodiment, the above solution is employed for a MAC (Message Authentication Code) algorithm change, resulting in a packet size change. Traditionally, for convenience the same RC4 key stream may be used in the generation of the keying material needed to calculate a MAC for each packet (a MAC is appended after the encrypted text). Where the MAC pad is key used to generate the MAC, for one-time use only. So, wehre a key stream is used for MAC generation (instead of or in addition to encryption) and the size of that random pad changes, one must rekey and start a new RC4 key stream in the same way as fro CODE changes”.

As to dependent claim 13, “further comprising: extracting the at least a portion of the received message digest value from the data packet; generating the locally generated message digest value based on the at least a portion of the received session count, a received encrypted payload of the data packet and a message digest key; truncating the locally generated message digest value to form a truncated message digest; and comparing the truncated message digest to the at least a portion of the received message digest value” is shown in ‘081 page 4, paragraph 4-5, paragraphs 0054-0057.

Art Unit: 2134

As to dependent claims 28-32, these claims contain substantially similar subject matter as claims 9-13; therefore they are rejected along the same rationale.

As to dependent claim 40, “further comprising: a message digest extractor configured to extract the at least a portion of the received message digest value from the received encrypted data packet” is taught in ‘081 page 4, paragraph 0054 “In a further embodiment, the above solution is employed for a MAC (message Authentication Code) algorithm change, resulting a in a packet size change”;

“a message digest generator configured to generate a locally generated message digest value based on the at least a portion of the session count, a received encrypted payload of the data packet and a message digest key” is shown in ‘081 pages 4-5 paragraph 0055-0056 “For example, additional key stream bytes may be allocated to calculate a MAC for each frame. However, ehre is only one MAC needed for the whole RTP packet and if an RTP packet contains multiple frames only the key stream bytes allocated to one of the frames ...

Where the MAC pad is a key used to generate the MAC, for one-time use only;

“a truncator configured to truncate the locally generated message digest value to form a truncated message digest; and a message digest evaluator configured to compare the truncated message digest value to the at least a portion of the received message digest value” is disclosed in ‘081 page 5, paragraph 0057 “one must rekey and start a new RC4 key stream in the same way as fro CODEC changes”;

“where the received is configured to discard the received encrypted data packed it the truncated message digest value does not match the at least a portion of the received message digest value” is taught in ‘012 page 5, paragraph 0052 “The key check block is sent to

the receiver as a header of the current encrypted data payload. The receiver also retains the last eight bytes of the current packet, it decrypted the first eight bytes (the key check block) and compares the result to the retained last eight bytes ... If there is no match, an error occurred and the receiver takes appropriate action”.

As to dependent claim 52, “further comprising discarding the data packet if the difference is not less than the threshold value” is taught in ‘012 page 5 paragraph 0052.

8. **Claims 54-57**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Medvinsky U.S. Patent Application Publication No. 2002/0094081 (hereinafter ‘081) in view of Sengodan et al. U.S. Patent 6,918,034 (hereinafter ‘034).

As to dependent claim 54, the following is not explicitly taught in ‘081: **“further comprising: padding the payload to a given size with padding, the given size corresponding to the fixed length segment size, wherein the fixed length segment of the continuous decryption key is applied to the padded payload, a remaining portion of the fixed length segment being applied to the padding”** however ‘034 teaches that padding is added to packets so that each packet is a predetermined block size in col. 4, lines 30-36.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method encryption/decryption utilizing stream ciphers over the Internet taught in ‘081 to include a means add padding to the exchanged packets. One of ordinary skill in the art would have been motivated to perform such a modification because there is a need to introduce padding at the packet level see ‘034 (col. 3, line 65 through col. 4, line 29). “Currently, there exist mechanisms for providing encryption at the IP level and at the RTP level. These mechanisms have taken into account the fact that block encryption schemes require the input to be an integral

Art Unit: 2134

multiple of the block size. This has been made possible by suitable padding schemes. However, in an environment where several mini-packets are multiplexed into a RTP packet, no suitable encryption (and corresponding padding) mechanism has been proposed ... It can be seen then that there is a need to provide padding and encryption on a mini-packet basis. It can also be seen that there is a need for a mechanism to perform padding and encryption at the mini-packet level. It can also be seen then that there is a need for a mechanism to perform authentication at the mini-packet level. To overcome the limitations in the prior art described above, and to overcome other limitations that will become apparent upon reading and understanding the present specification, the present invention discloses a method and apparatus to provide encryption and authentication of a mini-packet in a multiplexed real time protocol (RTP) payload. The present invention solves the above-described problems by providing a mechanism to perform padding, encryption and authentication at the mini-packet level”.

As to dependent claim 55, “further comprising: padding the data with padding; applying the fixed length segment to the padded data to form padded encrypted data, wherein a remaining portion of the fixed length segment is applied to the padding; and de-padding the padded encrypted data to form the encrypted payload” however ‘034 teaches how the padding is added and removed (de-padding) to authenticate and encryption of packets exchanged in col. 4, lines 30-61.

As to dependent claim 56, “further comprising: a padding engine operable to pad the data and coupled to supply the padded data to the encryption engine; and a pad remover coupled to receive encrypted padded data from the encryption engine and operable to remove the encrypted padding” however ‘034 teaches how the padding is added

Art Unit: 2134

and removed (de-padding) to authenticate and encryption of packets exchanged in col. 4, lines 30-61.

As to dependent claim 57, this claim contains substantially similar subject matter as claim 56; therefore it is rejected along similar rationale.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Ellen Tran
Patent Examiner
Technology Center 2134